

**Индивидуальный проект - 4**  
**Использование nikto**  
**Кузьмин Артем Дмитриевич**

## **Содержание**

<b>1 Цель работы</b>	<b>4</b>
<b>2 Введение</b>	<b>5</b>
2.1 Nikto: Описание	5
2.2 Полезные параметры и примеры	6
<b>3 Выполнение лабораторной работы</b>	<b>7</b>
3.1 Сканирование localhost	7
3.2 Сканирование localhost/dvwa/	9
<b>4 Вывод.</b>	<b>11</b>

# **1 Цель работы**

Целью данной работы является изучение сканера уязвимостей nikto.

## 2.1 Nikto: Описание

Nikto — это популярный сканер веб-серверов с открытым исходным кодом, который проверяет веб-серверы на наличие уязвимостей, неправильных настроек, устаревших версий ПО и прочих проблем безопасности. Основные задачи Nikto:

- Поиск общих уязвимостей веб-серверов.
- Проверка наличия опасных файлов и конфигураций.
- Выявление устаревших версий веб-серверов и их компонентов.
- Определение серверных технологий и модулей.

Особенности:

- Поддержка множества серверов и протоколов (HTTP, HTTPS, HTTP/2 и другие).
- Возможность добавления собственных правил для обнаружения уязвимостей.
- Регулярные обновления базы данных уязвимостей.

Nikto — это пассивный сканер, и он не пытается активно взламывать систему, а только собирает информацию о потенциальных уязвимостях. Рекомендуется использовать Nikto в сочетании с другими инструментами безопасности, такими как Nmap и OpenVAS, для более полного анализа безопасности веб-сервера.

## 2.2 Полезные параметры и примеры

Nikto написан на Perl, и для его работы необходимо наличие Perl на системе. Сканирование веб-сервера

```
perl nikto.pl -h
```

Сканирование определенного порта

```
perl nikto.pl -h -p
```

Вывод результатов в файл

```
perl nikto.pl -h -o output.txt
```

Дополнительные аргументы:

- -ssl — принудительное использование SSL (HTTPS).
- -no\_ssl — игнорирование SSL-сертификатов.
- -Tuning — настройка интенсивности сканирования (например, отключение проверки директорий).
- -Plugins — выбор определенных плагинов для сканирования.
- -timeout — установка таймаута для запросов

### 3 Выполнение работы

Nikto может использоваться для пассивного сканирования DVWA, выявления базовых уязвимостей и проверок на неправильную конфигурацию. Когда DVWA запущено, мы можем использовать Nikto для сканирования. Основной командой для сканирования будет:

perl nikto.pl -h <http://localhost/dvwa/>

```
(artemkuzmin@artem)-[~]
$ nikto -h http://localhost
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2025-03-16 13:41:57 (GMT3)

+ Server: Apache/2.4.63 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cf, size: 63141f9af8551, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ 7850 requests: 0 error(s) and 5 item(s) reported on remote host
```

Рис 1. Тестирование localhost

```
(artemkuzmin@artem)-[~]
$ nikto -h http://localhost/dvwa/
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2025-03-16 13:43:37 (GMT3)

+ Server: Apache/2.4.63 (Debian)
+ /dvwa/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /dvwa/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ 7849 requests: 0 error(s) and 3 item(s) reported on remote host
```

### 4 Вывод

В результате выполнения работы я повысил свои навыки использования приложений с целью информационной безопасности. Также познакомился с новым софтом под названием Nikto. Мощные инструменты задействованы в этом приложении.